DrinkerBiddle&Reath
LLP

Laura H. Phillips
202-842-8891
laura.phillips@dbr.com

Law Offices
1500 K Street, N.W.
Suite 1100
Washington, DC
20005-1209

202-842-8800
202-842-8465 fax
www.drinkerbiddle.com

PHILADELPHIA
NEW YORK
LOS ANGELES
SAN FRANCISCO
PRINCETON
FLORHAM PARK
BERWYN
WILMINGTON

July 1, 2004

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 Twelfth Street S.W.
Washington, D.C. 20554

Re: *Ex Parte* of RealNetworks, Inc. MB Docket No. 04-65;
In the Matter of Digital Output Protection Technology and
Recording Method Certifications, Helix DRM Trusted Recorder
and Helix Device DRM Technology

Dear Ms. Dortch:

RealNetworks, Inc. ("RealNetworks"), by its attorneys, hereby submits additional information in support of its pending certification application for interim authorization of Helix Device DRM (Digital Rights Management) Trusted Recorder and Helix Device DRM.

This submission responds both to a question from Federal Communications Commission ("Commission") staff about the authorization process for new devices as well as provides an update on the scope of proximity controls RealNetworks is prepared to apply to its interim authorization for protection of Broadcast Flag Marked Content from indiscriminate redistribution. RealNetworks hereby clarifies in response to a Commission staff question that the authorization of new devices is passive (*i.e.* automatic) and thus does not require any interaction or activity initiated by a Helix Device DRM user.

RealNetworks also provides additional information to the Commission on the dialogue between the MPAA parties and RealNetworks concerning matters of content protection and local proximity limitations.[1] One critical result of these discussions is agreement on the specific parameters defining Helix DRM's initial proximity content controls. RealNetworks and MPAA have agreed on the following initial proximity content control mechanisms and parameters to be applied to RealNetworks' interim Certification.

[1] This *ex parte* also responds directly to and resolves the National Football League's criticism that RealNetworks' Helix DRM and Helix Device DRM fail to appropriately protect the "localism" concerns of the National Football League with respect to its content. *See Ex Parte* of the National Football League, filed June 24, 2004, MB Docket No. 04-65.

Established
1849

At a minimum, Helix DRM's proximity detection will include: (i) setting the Internet Protocol (IP) packet header parameter Time to Live (TTL) to 3 in all transmitted IP packets of Helix DRM protected Marked Content output from a Trusted Recorder; (ii) confirmation that any IP packets of Helix DRM protected Marked Content received by a Trusted Client have an IP TTL parameter value of no greater than 3; and (iii) confirmation by the Trusted Recorder for any transmission of Helix DRM protected Marked Content (including over point-to-point wired connections) that one valid measurement of a Round Trip Time (RTT) of 7 milliseconds or less has been made between itself and the Trusted Client prior to completing the Trusted Client's authentication request.[2] TTL is defined in Internet Standard RFC 791 STD 5.

The measurement of RTT by a Trusted Recorder will occur: (a) after power-up of the Trusted Recorder when an active Trusted Client requests authentication; (b) when the last transmission of content-based packet traffic between a Trusted Recorder and a Trusted Client has occurred more than 120 minutes prior; and (c) when the last successful RTT measurement of 7 milliseconds or less between a Trusted Recorder and a Trusted Client has occurred more than 24 hours prior.

The determination of RTT will be measured using a cryptographically secure protocol to prevent any form of spoofing and to ensure that only the authenticating Trusted Client receiving the Helix DRM protected Marked Content can respond to the RTT measurement message. A Trusted Recorder will attempt the measurement of RTT until it achieves a single valid measurement of 7 or fewer milliseconds or determines that this requirement cannot be met and completion of authentication is halted. Thus, the RTT measurement will be the minimum RTT value measured and not the average of all RTT values measured.

The Helix DRM's proximity detection will be used during (i) the process of association of Trusted Clients to a single Trusted Recorder and (ii) the process of delivering Helix DRM protected Marked Content from a Trusted Recorder to a Trusted Client. In both cases, the Trusted Recorder will conduct proximity detection to confirm that the Trusted Client is proximate before completing the process.

[2] As explained in RealNetwork's April 16, 2004 Reply to Opposition, the term "Trusted Recorder" means Helix Device DRM technology software, and "Trusted Client" means a device that includes the Helix Device DRM client system and has been validated by a Trusted Recorder.

In order for a Trusted Client to consume Helix DRM protected Marked Content originating from a Trusted Recorder, it must associate itself with the Trusted Recorder and obtain the Recorder's Trusted Recorder Key. This association process may only be done if the Trusted Recorder confirms that the Trusted Client is proximate based on the proximity detection outlined above. Once this is confirmed, distribution of the Trusted Recorder Key occurs via the previously-described Trusted Recorder Protocol. The protocol registers the Trusted Client with the Trusted Recorder Key Group, as described below.

In addition to requiring proximity detection before distributing the Trusted Recorder Key, the Trusted Recorder will also restrict the distribution of Helix DRM protected Marked Content only to Trusted Clients that pass the proximity criteria outlined above. Before a Trusted Client can render a stream or download Helix DRM protected Marked Content, it must obtain an authenticated message from the Trusted Recorder indicating that it meets the proximity criteria and is a member of the same Trusted Recorder Key Group. When archiving Helix DRM protected Marked Content, the Trusted Client will modify the Marked Content, cryptographically binding it to the Trusted Client receiving it and indicating that the Marked Content was archived when the proximity criteria were met. When a Trusted Client attempts to consume Helix DRM protected Marked Content that it has archived, it must first validate that the Marked Content is bound to this particular Trusted Client and that it passed proximity criteria when it archived the Marked Content being consumed.

Another important feature of the Helix DRM is there is a limit on the number of Trusted Clients that can register and belong to a single Trusted Recorder Key Group. The Trusted Recorder Key Group consists of 10 Trusted Client seats. Each new registration of a Trusted Client results in a seat being occupied for a period of 6 months. At the end of 6 months, the Trusted Client will delete its Trusted Recorder Key and its seat in the Trusted Recorder Key Group will open again, allowing it to register again or a new Trusted Client to be registered. The deletion of the Trusted Recorder Key in the Trusted Client occurs automatically without a need for connecting to the Trusted Recorder. By ensuring that the Trusted Client deletes the Trusted Recorder Key, the number of Trusted Clients that can be registered to a single Trusted Recorder Key Group will never grow beyond 10.

Once a Trusted Client has deleted its Trusted Recorder Key, it will not be able to play recorded Helix DRM protected Marked Content until it has re-registered with the Trusted Recorder from which the Marked Content originated. A Trusted Client may only be registered with one Trusted Recorder at a time. Therefore, if a Trusted Client registers itself with a new Trusted Recorder, it loses any prior registration and erases the Trusted Recorder Key associated with the previous Trusted Recorder. Despite losing its registration with a particular Trusted Recorder Key Group, the seat occupied within the Trusted Recorder Key Group previously occupied by the departing Trusted Client will remain occupied for 6 months from the date the departing Trusted Client initially registered with the Trusted Recorder. This time latency in filling vacated seats addresses the issue of a Trusted Client switching many times between multiple Trusted Recorder Key Groups because its seats will be occupied in all of the Trusted Recorder Key Groups with which it registers. If a Trusted Client attempts to re-register while it still occupies a seat (i.e. within 6 months of last registration), the Trusted Client will be re-registered and its same seat will remain occupied for another 6 months; i.e., a Trusted Client will never occupy more than one seat with any Trusted Recorder Key Group within the same six month period, even though it may re-register with that Trusted Recorder Key Group more than once.

In addition to these proximity and key management controls, the Trusted Client software implementations are required at run-time to validate that either: a) the digital certificate to be used by the Trusted Client is appropriately and securely bound to the hardware device for which is was issued, or b) the hardware characteristics of the computer platform match the hardware characteristics to which the Trusted Client software itself was originally issued. This ensures that the Trusted Client software application will only enable the consumption of Helix DRM protected Marked Content on the hardware platform to which it was originally bound. This prevents the circumstance where a digital certificate or Trusted Client software module is simply distributed to many other computers that might then otherwise allow other computers to consume previously-archived Helix DRM protected Marked Content.

RealNetworks submits that these clarifications of its interim Certification permit the Commission to make a full evaluation of the suitability of Helix DRM and Helix Device DRM to protect Broadcast Flag Marked Content in a manner that is comprehensive and more far-reaching than that required under the Commission's rules. RealNetworks also confirms that it is in discussions with the MPAA parties on the future, further technological means of achieving proximity controls in the Helix Device DRM, as well as additional Compliance rules the MPAA parties have requested relating to the use and licensing of Helix Device DRM technology.

Respectfully submitted,

Laura Phillips

Laura H. Phillips
Counsel for RealNetworks, Inc.

cc: Steven Broeckaert
Rick Chessen
John Gabrysch
Alison Greenwald
Amy Nathan
Jeffrey Neumann
Susan Mort
Mary Beth Murphy
Alan Stillwell